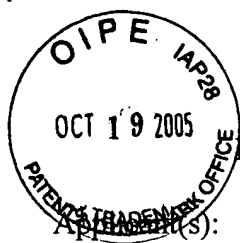


AF-3621
ZPW



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Jeffrey N. Sloan, Gary W. Cobb

Assignee: Dell Products L.P.

Title: Verification of a Benefit Purchase Incident to a Computer System Purchase

Serial No.: 09/768,434

Filing Date: January 24, 2001

Examiner: John W. Hayes

Group Art Unit: 3621

Docket No.: DC-02638

Customer No.: 33438

Austin, Texas
October 14, 2005

Mail Stop Appeal Brief - Patents
Board of Patent Appeals and Interferences
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL APPEAL BRIEF UNDER 37 CFR § 41.37

Dear Sir:

Applicant submits this Supplemental Appeal Brief pursuant to the Office Action dated September 14, 2005. No additional fee is believed to be required; however, the Board is authorized to deduct any amounts required for this supplemental appeal brief and to credit any amounts overpaid to Deposit Account No. 502264.

I. REAL PARTY IN INTEREST - 37 CFR § 41.37(c)(1)(i)

The real party in interest is the assignee, Dell Products, L.P., as named in the caption above and as evidenced by the assignment set forth at Reel 011520, Frame 0141.

II. RELATED APPEALS AND INTERFERENCES - 37 CFR § 41.37(c)(1)(ii)

Based on information and belief, there are no appeals or interferences that could directly affect or be directly affected by or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal.

III. STATUS OF CLAIMS - 37 CFR § 41.37(c)(1)(iii)

Claims 1 - 20 are pending in the application. Claims 1 - 20 stand rejected. The rejection of Claims 1 - 20 is appealed. Appendix "A" contains the full set of pending Claims.

IV. STATUS OF AMENDMENTS - 37 CFR § 41.37(c)(1)(iv)

No amendments after final have been requested or entered.

V. SUMMARY OF CLAIMED SUBJECT MATTER - 37 CFR § 41.37(c)(1)(v)

The present invention, as set forth by independent Claim 1, relates to a method for purchase verification (e.g., 400, 500), comprising the acts of receiving at a server a first message from a computer system (e.g., 410), determining at the server if the service tag is valid (e.g., 502), and generating a second message from the server (e.g., 508). The first message includes a service tag which uniquely identifies the computer system (see e.g., application page 8, line 28 – page 9, line 5.). The second message authorizes providing a benefit if the service tag is determined to be valid.

The present invention, as set forth by independent Claim 4, relates to a method for purchase verification (e.g., 400, 500), comprising the acts of generating a service tag that uniquely identifies a computer system, the computer system including a processor coupled to a memory, storing the service tag in the memory at assembly of the computer system (see e.g., application, page 9, lines 21 - 29.), receiving a message at a server sent from the computer system (e.g., 410), the message including the service tag, verifying that the service tag value as received matches a service tag value stored in the server (e.g., 502, 506), and authorizing receipt of a benefit if the received service tag matches (e.g., 508).

The present invention, as set forth by independent Claim 8, relates to a method for purchase verification of a benefit (e.g., 400, 500), comprising the acts of receiving a first message at a first server (e.g., 312, 410), transmitting a second message from the first server to a second server (e.g., 420) and transmitting from the second server a third message to the first server (e.g., 450). The first message being sent from a computer system and includes a service

tag which uniquely identifies a computer system. The second server attempts to verify the validity of the service tag. The third message allows access to the benefit.

The present invention, as set forth by independent Claim 11, relates to a system in a computer system (e.g., 130) for purchase verification (e.g., 400, 500), the computer system includes a processor. The system includes a non-volatile computer readable memory. The non-volatile computer readable memory includes instructions, executable on the processor, configured to store a service tag installed upon assembly of the computer system (see e.g., application, page 9, lines 21 – 29), the service tag uniquely identifying the computer system; and instructions, executable on the processor, configured to send the service tag to a remote server to verify purchase of a benefit (e.g., 312).

The present invention, as set forth by independent Claim 14, relates to a system for purchase verification (e.g., 300, 400), the system being on a server platform, the server operated by a service provider (e.g., 220), the server configured to communicate with a purchased computer system (e.g., 130), the server including a processor and a memory, the server platform configured to communicate with a remote computer system. The system includes a non-volatile computer readable memory. The non-volatile computer readable memory storing a database, the database (e.g., 232) including a set of valid service tags which correspond to computer systems that purchased a benefit, and instructions, executable on the processor, configured to receive a message (e.g., 410), the message including a service tag which uniquely identifies a computer system.

VI. GROUND S OF REJECTION TO BE REVIEWED ON APPEAL - 37 CFR § 41.37(c)(1)(vi)

Claims 1, 14 and 17 – 19 stand rejected under Challener et al, U.S. Patent No. 6,654,886 B1 (Challener). Apparently Claims 15 and 16 also stand rejected under 35 U.S.C. §102(e) over Challener although this rejection has not been specifically stated by the Examiner.

Claims 2 – 3 and 8 – 10 stand rejected under 35 U.S.C. § 103 over Challener. Apparently Claim 20 also stands rejected under 35 U.S.C. § 103 over Challener although this rejection has not been specifically stated by the Examiner.

Claims 4 – 7 and 11 – 13 stand rejected under Challenger in view of Colligan et al., GB 2339488 (Colligan).

VII. ARGUMENT - 37 CFR § 41.37(c)(1)(vii)

Claims 1 and 14 – 19 are allowable over Challenger.

In general, the present invention relates to enabling a benefit purchase incident to the purchase of a computer system by verifying the benefit based upon a service tag that is embedded within the computer system at the time of manufacture of the computer system. The value of the service tag uniquely identifies a computer system and is installed in the basic input/output system (BIOS) of the computer system. Storing the service tag in the system BIOS prevents the service tag from being lost such as when the hard disk is reformatted.

When discussing service tags, the application sets forth:

The service tag, for instance, is an alpha-numeric field of varying length, typically less than 64 characters. The value of the service tag uniquely identifies the computer system and is akin to a serial number. In one embodiment, a unique service tag is associated with each computer system 130 with which pre-paid goods or services may be purchased regardless of whether such goods or services are actually purchased when computer system 130 is ordered from the manufacturer. (Application, page 8, line 31 – page 9, line 5.)

When discussing a service tag, the application also sets forth:

The service tag is installed in the system memory. Specifically, the service tag can be installed in the basic input/output system (BIOS) which itself is stored in non-volatile memory in the computer. Storing the service tag in the system BIOS prevents the service tag from being lost if the hard disk is formatted. (Application, page 10, lines 21 – 24.)

More specifically, the present invention, as set forth by independent Claim 1, relates to a method for purchase verification, comprising the acts of receiving at a server a first message from a computer system, determining at the server if the service tag is valid, and generating a second message from the server. The first message includes a service tag which uniquely identifies the computer system. The second message authorizes providing a benefit if the service tag is determined to be valid.

The present invention, as set forth by independent Claim 14, relates to a system for purchase verification, the system being on a server platform, the server operated by a service provider, the server configured to communicate with a purchased computer system, the server including a processor and a memory, the server platform configured to communicate with a remote computer system. The system includes a non-volatile computer readable memory. The non-volatile computer readable memory storing a database, the database including a set of valid service tags which correspond to computer systems that purchased a benefit, and instructions, executable on the processor, configured to receive a message, the message including a service tag which uniquely identifies a computer system.

When discussing Claim 1, the Examiner set forth

As per Claim 1, Challener et al discloses a method for purchase verification, comprising the acts of:

- receiving at a server a first message from a computer system, the first message including a service tag, the first message including a service tag, the service tag uniquely identifying the computer system (Col. 3, lines 5-25; Col. 5, lines 64-65 Col. 6, lines 10-20);
- determining at the server if the service tag is valid (Col. 3, lines 9-15; Col. 6, lines 10-25; Col. 6 line 62-Col. 7 line 1); and
- generating a second message from the server, the second message authorizing providing a benefit if the service tag is determined to be valid (Col. 7, lines 1-5). (Final Office action, page 4.)

When discussing Claim 14, the Examiner set forth

As per Claim 14, Challener et al discloses a system for purchase verification, the system being on a server platform (Figure 1), the server operated by a service provider (Col. 3, lines 20-25), the server configured to communicate with a purchased computer system (Figure 1), the server including a processor and a memory, the server platform configured to communicate with a remote computer system (Figure 1), the system comprising:

- a non-volatile computer readable memory, the non-volatile computer readable memory storing:
 - a database, the database including a set of valid service tags, the valid service tags corresponding to computer systems that purchased a benefit (Col. 3, lines 1-13; Col. 6, lines 1-15); and
 - instructions, executable on the processor, configured to receive a message, the message including a service tag, the service tag uniquely identifying a computer system (Col. 3, lines 5-25; Col. 6, lines 1-5). (Final Office action pages 3, 4.)

In Response to the Arguments relating to Claim 4 submitted on October 4, 2004, the Examiner set forth:

With respect to Claim 14, applicant argues that the references fail to disclose the valid service tag corresponding to computer systems that purchased a benefit. Examiner respectfully disagrees and submits that Challenger et al, as discussed above, discloses the storage of valid service tags in the form of preregistered log-in tokens which are used to approve the utilization of a service such as access to Internet service or access to warranty service. (Final Office action, Page 2.)

Challener discloses a method for permitting only a pre-registered client computer to access a service executing on a server. A log-in token is established including a unique identifier which identifies a particular client computer. The client computer logs-on to the server. Subsequent to the client computer logging-on to the server, the client computer attempts to access the service. During the attempt, the client computer transmits the log-in token to the server. The server uses the unique identifier included within the log-in token to determine if the client computer is registered to access the service. In response to a determination that the client computer is registered to access the service, the server permits the client computer to access the service. In response to a determination that the client computer is not registered to access the service, the server prohibits the client computer from accessing the service.

More specifically, Challener sets forth:

The present invention is a method and system for permitting only preregistered client computer hardware to access a service executing on a remote server computer system. The client computer hardware first log-on to the server executing the service. Then, the client computer hardware registers with the service once the service has been purchased for the particular client hardware. The client hardware registers by transmitting an initial log-in token to the service. The service stores the initial log-in token in an access registry. Therefore, the access registry identifies all preregistered, pre-approved hardware which may access the service (Challener Col. 2, line 63-Col. 3, line 6).

When generally discussing subsequent attempts to access a server, Challener sets forth:

Thereafter, during subsequent attempts to access the service, the client hardware will transmit a log-in token to the service. The log-in token will be received by the service and compared to the contents of the access registry. If the log-in token matches any of the contents of the registry, the service will transmit an approval to the client hardware to access the service (Challener Col. 3, lines 7-13).

The initial log-in token and subsequent log-in tokens include a unique identifier which identifies particular client hardware. The unique identifier may be a serial number for the hardware, contract number, warranty number, or any other identifier which uniquely identifies particular hardware (Challener Col. 3, lines 14-19).

Thus, Challenger requires both an initial log-in during which a log-in token is generated (i.e., during which pre-registration occurs) as well as subsequent log-ins during which the generated log-in token is used. The log-in token generated during the initial log-in is then used for subsequent logging into the service.

Challenger does not disclose or suggest a purchase verification method which uses a service tag as Claimed by both independent Claims 1 and 14. Applicant's submit that log-in tokens as set forth by Challenger do not disclose or suggest the use of service tags as defined and used in the application and Claims of the present application.

More specifically, when discussing generating and transmitting a log-in token Challenger sets forth:

The process starts as depicted at block 400 and thereafter passes to block 402 which illustrates purchasing a service for a particular client hardware. The particular client hardware becomes associated with the server after the purchase of the service. Next, block 404 depicts the client computer system *generating an initial log-in token for a particular client hardware*. The token includes the unique identifier which identifies the particular client computer hardware. (Challenger, Col. 5, lines 57 –65, emphasis added.)

Thereafter, block 406 illustrates the client *signing the initial log-in token by encrypting the token utilizing the client's private key*. Next, block 408 depicts the client transmitting the encrypted initial log-in token to the server for the service to store in its access registry. The process then terminates as illustrated at block 410. (Challenger, Co. 5, line 66 – Col. 6, line 4, emphasis added.)

Figure 4 of Challenger shows:

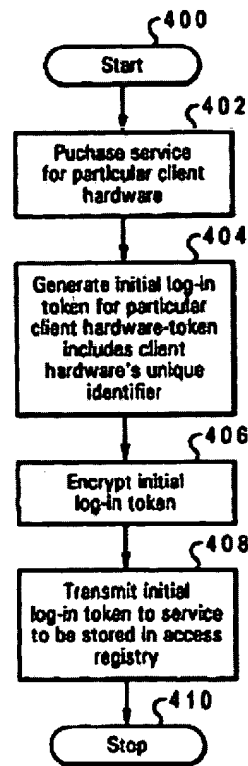


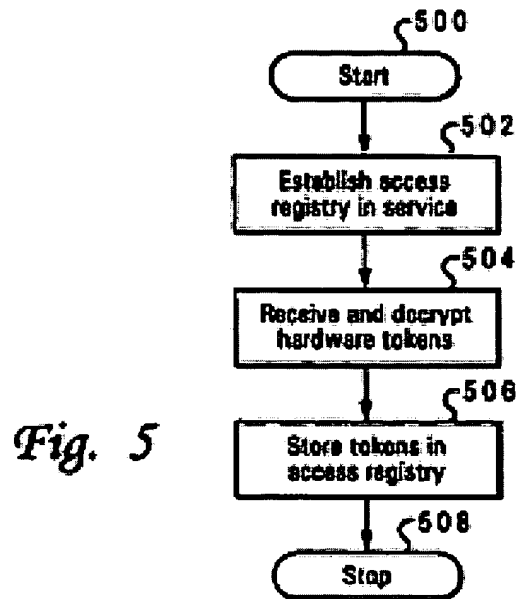
Fig. 4

When discussing a service establishing an access registry within a service, Challenger sets forth:

The process starts as depicted at block 500 and thereafter passes to block 502 which illustrate the service establishing an access registry within the service. The access registry is utilized by the service to store all *preregistered log-in tokens which identify the particular client computer hardware which are approved to utilize the service.* (Challener Col. 5, lines 57-65, emphasis added.)

Next, block 504 depicts the service, executing within the server, authenticating the client by receiving and *decrypting initial log-in tokens.* Thereafter, block 506 illustrates *the service storing the decrypted tokens in the access registry.* **Once** a log-in token has been received and stored within the access registry, the client hardware is associated with the token is registered and approved to log-on to and access the service. The process then terminates as depicted at block 508 (Challener Col. 5, line 66-Col. 6, line 4, emphasis added.)

Figure 5 of Challenger shows:



When discussing a client computer system accessing a service, Challenger sets forth

FIG. 6 depicts a high level flow chart which illustrates a client computer system attempting to access a service executing on a remote server by transmitting the client's log-in token in accordance with the method and system of the present invention. The process starts as illustrated at block 600 and thereafter passes to block 602 which depict the client computer system loading its operating system. Next, block 604 illustrates the client computer hardware logging-on to the server computer system. Thereafter, block 606 depicts the client encrypting its log-in token utilizing the client's private key and server's public key. (Challenger Col. 6, lines 5-15, emphasis added.)

The process then passes to block 608 which illustrates the client transmitting its encrypted log-in token to the server computer system. Block 610, then, depicts a determination of whether or not the client computer hardware has received an approval to log-on to and access the service. If a determination is made that the client computer hardware has received an approval, the process passes to block 612 which illustrates the client computer hardware being permitted to log-on to and utilize the service. The process then terminates as depicted at block 614. Referring again to block 610, if a determination is made that the client computer hardware is not permitted to log-on to the service, the process terminates at block 614 (Challenger Col. 6, lines 16-24).

Figure 6 of Challenger shows:

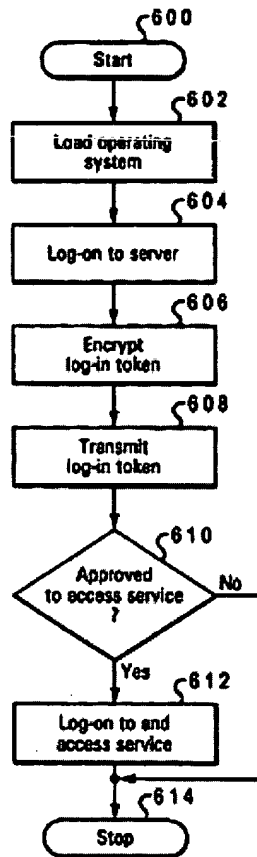


Fig. 6

When discussing a server system receiving a log-in token, Challenger sets forth:

Next, block 708 depicts a determination of whether or not the *received, decrypted token* matches any of the initial tokens stored in the access registry. If a determination is made that the received log-in token does match one of the stored initial tokens, then the *client computer hardware identified by the token is pre-approved to access and utilize the service*. Block 712, then, illustrates the service transmitting an approval to the client computer hardware identified by the log-in token to utilize the service. The process then terminates as illustrated at block 710. Referring again to block 708, if a determination is made that the service is not able to match the received token to any token stored in the access registry, then the client hardware identified by the token is not registered to utilize the service. Therefore, the process terminates at block 710. (Challenger Col. 6, line 62-Col. 7, line 9, emphasis added.)

Figure 7 of Challenger shows:

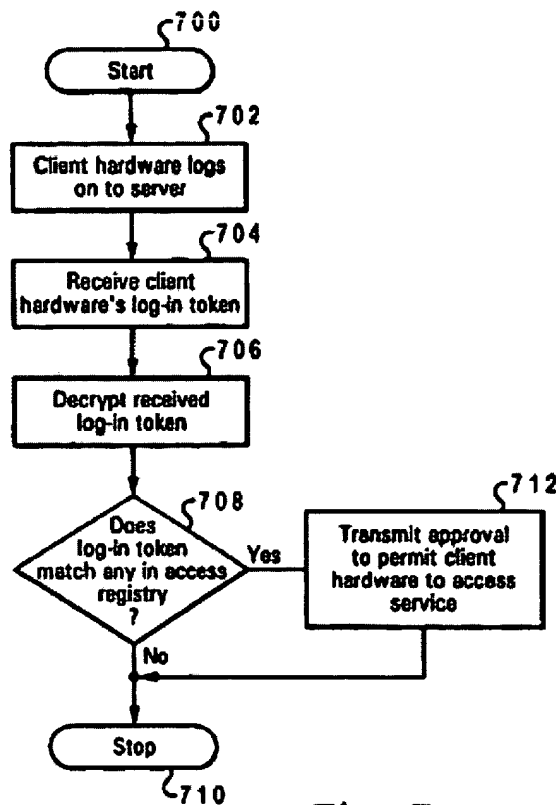


Fig. 7

Accordingly, Challenger does not disclose or suggest a purchase verification method which uses a service tag as Claimed by both independent Claims 1 and 14.

More specifically, Challenger, taken alone or in combination, does not teach or suggest a method for purchase verification which includes *determining at the server if the service tag is valid*, and generating a second message which authorizes providing a benefit *if the service tag is determined to be valid*, all as required by Claim 1. Accordingly, Claim 1 is allowable over Challenger.

Additionally, Challenger, taken alone or in combination, do not teach or suggest a system for purchase verification which is on a server platform and includes a computer readable memory storing a database, the database including a set of valid service tags, *the valid service tags corresponding to computer systems that purchased a benefit*, and instructions, executable on a processor of the server, configured to receive a message, the message including *a service tag*, all as required by Claim 14. Accordingly, Claim 14 is allowable over Challenger.

Additionally, Challenger does not disclose or suggest certain features of Claims 15 – 19. More specifically, Challenger does not disclose or suggest receiving a message which includes a product code (in addition to the service tag) as required by Claim 15; authorizing a purchaser to receive a benefit as required by Claim 16; verifying the service tag where the verifying includes receiving the service tag from the computer system, recalling the service tag stored in the server and comparing the service tag received from the computer system to the service tag recalled from the server to determine if the service tag received from the computer system matches the service tag recalled from the server as required by Claim 17; authorizing a purchaser to receive a benefit if the service tag received from the computer system matches the service tag recalled from the server as required by Claim 18; or, establishing an internet service provider service account if the service tag received from the computer system matches the service tag recalled from the server as required by Claim 19.

Claims 2 – 3 and 8 – 10 are allowable over Challenger.

The present invention, as set forth by independent Claim 8, relates to a method for purchase verification of a benefit, comprising the acts of receiving a first message at a first server, transmitting a second message from the first server to a second server and transmitting from the second server a third message to the first server. The first message being sent from a computer system and includes a service tag which uniquely identifies a computer system. The second server attempts to verify the validity of the service tag. The third message allows access to the benefit.

When discussing Claim 8, the Examiner set forth

As per Claim 8, Challenger et al discloses a method for purchase verification, comprising the acts of:

- receiving a first message at a first server, the first message being sent from a computer system, the first message including a service tag, the service tag uniquely identifying a computer system (Col. 3, lines 5-25; Col. 5, lines 64-65 Col. 6, lines 10-20); and

- transmitting a message allowing access to the benefit (Col. 7, lines 1-5).

Challener et al, however, fails to explicitly disclose a transmitting a second message from the first server to the second server, the second server attempting to verify the validity of the service tag. Examiner takes official notice that using a second server or even a third party server for validating tokens or other items used for identification purposes was well known in the art at the time of applicant's invention. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to modify the method of Challener et al and include using a second server for the specific purpose of validating a token or other item used for identification purposes. One would have been motivated to use a second server for validation procedures in order to reduce the necessary processing conducted by the primary server. (Final Office action, Page 7.)

When discussing Claims 2 and 10, the Examiner set forth:

As per Claims 2 and 10, Challener et al fail to specifically disclose invalidating the service tag after generating the second message. However, takes office notice that invalidating access to a service when it has been depleted was well known in the art at the time of applicant's invention. Challener et al describes that the service being accessed by the client may be any type of service for which access needs to be controlled (Col. 3, lines 20-25). Examiner submits that it was well known in the art to invalidate a token or other identifier after the client no longer met the requirements for access. Thus, it would have been obvious to one or ordinary skill in the art at the time of applicant's invention to modify the method of Challener et al and invalidate the client's log-in token in cases where the client has accessed a one time service or has otherwise depleted the allowed access. The motivation would be to ensure that the service tag or token cannot be used again and thereby reduce the possibility of fraud. (Final Office action, Page 6.)

When discussing Claims 3 and 9, the Examiner set forth:

As per Claims 3 and 9, Challener et al further discloses that the message includes a product code such as a service (Col. 1, lines 35-55; Col. 2 line 6; Col. 3, lines 20-25). (Final Office action, Page 6.)

When discussing Claim 20, the Examiner set forth

As per Claim 20, Challener fails to specifically disclose invalidating the service tag after generating the second message. However, takes official notice that invalidating access to a service when it has been depleted was well known in the art at the time of applicant's invention. Challener et al described that the service being accessed by the client may be any type of service for which access needs to be controlled (Col. 3, lines 20-25). Examiner submits that it was well known in the art to invalidate a token or other identifier after the client no longer met the requirements for access. Thus, it would have been obvious to one of ordinary skill in the art at the time of applicant's invention to

modify the method of Challener et al and invalidate the client's log-in token in cases where the client has accessed a one time service or has otherwise depleted the allowed access. The motivation would be to ensure that the service tag or token cannot be used again and thereby reduce the possibility of fraud.

As discussed in detail above, Challenger does not disclose or suggest a purchase verification method which uses a service tag as Claimed by independent Claim 8. Applicant's submit that log-in tokens as set forth by Challener do not disclose or suggest the use of service tags as defined and used in the application and Claims of the present application.

More specifically, Challener, taken alone or in combination, does not teach or suggest a method for purchase verification of a benefit, comprising receiving a first message at a first server, transmitting a second message from the first server to a second server and transmitting from the second server a third message to the first server where the first message is sent from a computer system and includes *a service tag, the second server attempts to verify the validity of the service tag, and the third message allows access to the benefit*, all as required by Claim 8. Accordingly, Claim 8 is allowable over Challener.

Additionally, Challener does not disclose or suggest certain features of Claims 2 and 3. More specifically, Challener does not disclose or suggest invalidating a service tag after generating a second message as required by Claim 2 or the first message including a product code (in addition to a service tag) as required by Claim 3.

Additionally, Challener does not disclose or suggest certain features of Claims 9 and 10. More specifically, Challener does not disclose or suggest the first message including a product code (in addition to a service tag) as required by Claim 9 or invalidating the service tag on the second server as required by Claim 10.

Additionally, Challener does not disclose or suggest certain features of Claim 20. More specifically, Challener does not disclose or suggest invalidating the service tag stored in the memory of the server as required by Claim 20.

Claims 4 – 7 and 11 – 13 are allowable over Challenger in view of Colligan.

The present invention, as set forth by independent Claim 4, relates to a method for purchase verification, comprising the acts of generating a service tag that uniquely identifies a computer system, the computer system including a processor coupled to a memory, storing the service tag in the memory at assembly of the computer system, receiving a message at a server sent from the computer system, the message including the service tag, verifying that the service tag value as received matches a service tag value stored in the server, and authorizing receipt of a benefit if the received service tag matches.

The present invention, as set forth by independent Claim 11, relates to a system in a computer system for purchase verification, the computer system includes a processor. The system includes a non-volatile computer readable memory. The non-volatile computer readable memory includes instructions, executable on the processor, configured to store a service tag installed upon assembly of the computer system, the service tag uniquely identifying the computer system; and instructions, executable on the processor, configured to send the service tag to a remote server.

When discussing Colligan, the Examiner set forth:

The reference to Colligan et al was merely used to show that it was known to store a unique computer identifier in the memory of a computer during assembly and to use this identifier to access some benefit.

Colligan discloses a protection technique that prohibits loading of a software image onto any computer hardware other than the computer hardware keyed to receive the software image. Reloading of the software image contained on a customer programmed CD ROM onto a hard disk drive of the computer is allowed only for a matched combination of a specific cross keyed customer programmed CD ROM, a specific associated bootable diskette and a uniquely keyed computer system. The uniquely keyed computer system is based upon, in part, the service tag of the computer system. Colligan sets forth that the service tag identifier specifically identifies a single computer. The service tag is typically a multiple character alphanumeric string that is programmed into a section of storage within the computer. In some systems, the service tag is stored within a hidden section of the nonvolatile memory during the manufacturing of the computer.

When discussing Claims 4 and 5, the Examiner set forth

As per Claims 4-5, Challener et al discloses a method for purchase verification, comprising the acts of:

- generating a service tag that uniquely identifies a computer system, the computer system including a processor coupled to a memory (Figure 2; Col. 3, lines 7-24; Col. 5, lines 45-50 and 60-65);
- receiving a message at a server sent from the computer system, the message including the service tag (Col. 3, lines 5-10; Col. 6, lines 1-5);
- verifying that the service tag value as received matches a service tag value stored in the server (Col. 3, lines 9-24; Col. 6, line 61-Col. 7 line 5);
- authorizing receipt of a benefit if the received service tag matched (Col. 3, lines 9-24; Col. 6, lines 40-45; Col. 6 line 61-Col. 7 line 5).

In response to the Arguments relating to Claim 4, the Examiner set forth:

With respect to Claim 4, applicant argues that Laor, Challener and Colligan, taken alone or in combination, do not teach or suggest a method for purchase verification which includes receiving a message at a server sent from the computer system, *the message including the service tag, verifying that the service tag value as received matches a service tag value stored in the server, and authorizing receipt of a benefit if the received service tag matches*. Examiner respectfully disagrees and notes that only the references to Challener et al and Colligan et al were used in the rejection of Claim 4. Examiner further submits that Challener et al discloses the subject matter recited in italics above. Challener discloses receiving a message at a server sent from the computer system, the message including the service tag in the form of a log-in token that uniquely identifies the client computer (Col. 3, lines 5-10; Col. 6, lines 1-15); verifying that the service tag value as received matches a service tag value or log-in token stored in the server (Col. 3, lines 9-24; Col. 6, lines 40-45; Col. 6 line 61-Col. 7 line 5) and authorizing receipt of a benefit if the received service tag matches (Col. 3, lines 9-24; Col. 6, lines 40-45; Col. 6 line 61-Col. 7 line 5).

When discussing Claim 11, the Examiner set forth

Challener et al, however fail to explicitly disclose storing the service tag in the memory at assembly of the computer system. Colligan et al discloses a system for downloading custom software to a unique computer and only authorizes the software to be downloaded if the computer is identified by the correct unique service tag (Page 4, lines 15-24; Page 5, lines 5-13; Page 9, lines 15-17; Page 10, lines 1-11). Colligan et al further discloses that the unique identifier for the specific computer is known as a service tag and is “burned” into a hidden section of non volatile memory such as the BIOS within the computer during the manufacturing process of the computer (Page 10, lines 6-11; Page 13, lines 7-22). It would have been obvious to one of ordinary skill in the art at the time of applicant’s invention to modify the method of Challener et al and utilize a unique identifier or service tag which is burned into non-volatile memory in order to uniquely identify the compute requesting services as taught by Colligan. One would have been motivated to use this type of identifier since it is an effective means for uniquely

identifying a specific computer to ensure that the identified computer is the one authorized to receive any type of service, access or software download.

In response to the Arguments relating to Claim 11, the Examiner set forth:

With respect to Claim 11, applicant argues that the references fail to disclose sending the service tag to a remote server to verify the purchase of a benefit. Examiner respectfully disagrees and submits that Challener et al discloses this feature (Col. 3, lines 5-10; Col. 6, lines 1-5). The log-in token transmitted to the remote server is used to verify purchase of a benefit such as access to Internet service or access to warranty service.

As discussed in detail above, Challenger does not disclose or suggest a purchase verification method which uses a service tag as Claimed by independent Claims 4 and 11. Applicant's submit that log-in tokens as set forth by Challener do not disclose or suggest the use of service tags as defined and used in the application and Claims of the present application. Additionally, merely replacing the log-in tokens as set forth by Challener with a service tag as disclosed by Colligan does not disclose or suggest the invention as Claimed.

More specifically, Challener and Colligan, taken alone or in combination, do not teach or suggest a method for purchase verification which includes receiving a message at a server sent from the computer system, *the message including the service tag, verifying that the service tag value as received matches a service tag value stored in the server, and authorizing receipt of a benefit if the received service tag matches*, all as required by Claim 4. Accordingly, Claim 4 is allowable over Challener and Colligan.

Challener and Colligan, taken alone or in combination, do not teach or suggest a system in a computer system for purchase verification having a non-volatile computer readable memory which includes instructions, executable on the processor, configured to store a service tag installed upon assembly of the computer system, the service tag identifying the computer system; and instructions, executable on the processor, configured to *send the service tag to a remote server to verify the purchase of a benefit*, all as required by Claim 11. Accordingly, Claim 11 is allowable over Challener and Colligan.

Additionally, Challener and Colligan do not disclose or suggest certain features of Claims 5 - 7. More specifically, Challener and Colligan do not disclose or suggest a service tag used as Claimed where the service tag is stored as part of a computer system BIOS as required by Claim 5; a second message authorizing a purchaser to receive the benefit if the service tag matches as

required by Claim 6; or, the benefit being an Internet Service Provider service as required by Claim 7.

Additionally, Challener and Colligan do not disclose or suggest certain features of Claims 12 and 13. More specifically, Challener and Colligan do not disclose or suggest storing a product code identifying a benefit as required by Claim 12 or communicating with a remote server having the ability to verify the service tag as required by Claim 13.

The combination of Challener and Colligan is improper

The combination of Challener and Colligan is improper because Challener and Colligan are nonanalogous prior art and because Challener and Colligan fail to provide a suggestion to be combined.

Challener and Colligan are nonanalogous prior art because Challener relates to permitting access to a service executing on a server and Colligan relates to prohibiting loading of a software image on to a computer.

The combination of elements from non-analogous sources, in a manner that reconstructs the applicant's invention only with the benefit of hindsight, is insufficient to present a *prima facie* case of obviousness. There must be some reason, suggestion, or motivation found in the prior art whereby a person of ordinary skill in the field of the invention would make the combination. That knowledge can not come from the applicant's invention itself *In re Oetiker*, 977 F.2d 1443, 24 USPQ 2d, 1443, 1446 (Fed. Cir. 1992)

Additionally, even if Challener and Colligan are found to be within analogous arts, neither Challener nor Colligan provide a suggestion for such a combination.

The mere fact that the prior art may be modified in the manner suggested by the Examiner does not make the modification obvious unless the prior art suggested the desirability of the modification. Wilson and Hendrix fail to suggest any motivation for, or desirability of, the changes espoused by the Examiner and endorsed by the Board.

Here, the Examiner relied upon hindsight to arrive at the determination of obviousness. It is impermissible to use the Claimed invention as an instruction manual or "template" to piece together the teachings of the prior art so that the Claimed invention is rendered obvious. This court has previously stated that "[o]ne cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the Claimed

invention. *In re Fritch*, 23 USPQ 2d at 1783-84 (quoting *In re Fine*, 837 F.2d 1071, 1075, 5 USPQ 2d 1596, 1600 (Fed. Cir. 1988)).

In response to the Argument that the combination of Challener and Colligan was improper, the Examiner set forth:

In response to applicant's argument that Colligan et al and Challener et al are nonanalogous art, it has been held that a prior art reference must either be in the field of applicant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the applicant was concerned, in order to be relied upon as a basis for rejection of the Claimed invention. See *In re Oetiker*, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992). In this case, both Challener et al and Colligan et al are reasonably pertinent to the particular problem with which the applicant was concerned since they both relate to accessing a benefit based on the identification of a client computer. Challener et al uses a log-in token to identify the client computer and Colligan et al uses a service tag to identify the computer and Examiner submits that one having ordinary skill in the art would look to other methods for identifying a client computer such as that taught by Colligan et al. Examiner submits that it would have been obvious to one having ordinary skill in the art to modify the teachings of Challener et al and utilize a service tag to identify the client computer instead of the log-in token as taught by Challener et al.

Applicants respectfully submit that neither Challener nor Colligan provide a suggestion for the combination provided by the Examiner.

The combination of Challener and Colligan is based upon an improper hindsight based analysis

The rejection of Claims 1 – 20 is based on an improper hindsight-based obviousness analysis. In this regard, it must be recognized that hindsight reconstruction of Claims based on disparate aspects of the prior art may not be employed as a valid basis for the rejection of those Claims. *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 220 USPQ 303, 312-313 (Fed. Cir. 1983); *Panduit Corp. v. Dennison Manufacturing Co.*, 1 USPQ2d 1593, 1595-1596 (Fed. Cir. 1987). Furthermore, an obviousness determination requires that the invention *as a whole* would have been obvious to a person having ordinary skill in the art. *Connell v. Sears Roebuck & Co.*, 220 USPQ 193 (Fed. Cir. 1983).

In response to the Argument that the combination of Challener and Colligan was improper, the Examiner set forth:

Furthermore, in response to applicant's argument that the Examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any

judgment of obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the Claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971).

To establish obviousness based on a combination of elements disclosed in the prior art or a modification of the prior art, there must be some motivation, suggestion or teaching of the desirability of making the Claimed invention. See *In re Dance*, 48 USPQ2d 1635, 1637 (Fed. Cir. 1998); *In re Gordon*, 221 USPQ 1125, 1127 (Fed. Cir. 1984). The motivation, suggestion or teaching to modify references may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some cases, the nature of the problem to be solved. *In re Dembiczak*, 50 USPQ2d 1614, 1617 (Fed. Cir. 1999). Whether the Office Action relies on an express or implicit showing of a motivation or suggestion to modify or combine references, it must provide particular findings related thereto. *In re Dembiczak*, 50 USPQ2d at 1617. Broad conclusory statements standing alone are not "evidence." *Id.* Thus, the Office Action must include particular *factual findings* that support an assertion that a skilled artisan would have modified the express disclosure of Challener and Colligan to develop the invention recited by independent Claims 1, 4, 8, 11, and 14. See *In re Kotzab*, 55 USPQ2d 1313, 1317. Applicant is unable to discern the requisite factual basis in Challener and Colligan or the Office Action.

In this regard, the Office Action has engaged in a hindsight-based obviousness analysis condemned by the Federal Circuit. To prevent a hindsight-based obviousness analysis, the Federal Circuit has clearly established that the relevant inquiry for determining the scope and content of the prior art is whether there is a reason, suggestion, or motivation in the prior art or elsewhere that would have led one of ordinary skill in the art to combine or modify references. See *Ruiz v. A.B. Chance Co.*, 57 USPQ2d 1161, 1167 (Fed. Cir. 2000); see also *In Re Rouffet*, 47 USPQ2d 1453, 1459 (Fed. Cir. 1998) ("[T]he Board must identify specifically ... the reasons one of ordinary skill in the art would have been motivated to select the references and combine them to render the Claimed invention obvious."). Applicant can detect, and the Examiner has pointed to, no motivation or suggestion that would prompt someone of ordinary in the art to look to Challener and Colligan in combination for a solution to the problem addressed by Applicant's invention. Such a determination that there is a suggestion or motivation to modify Challener and

Colligan is a factual finding that is prerequisite to an ultimate conclusion of obviousness. *Sibia Neurosciences, Inc. v. Cadus Pharma. Corp.*, 55 USPQ2d 1927, 1931 (Fed. Cir. 2000). Applicant respectfully submits that the Office Action is devoid of such a finding.

Without such a finding, a *prima facie* case of obviousness in rejecting Claims 1 – 20 under 35 U.S.C. § 103(a) based on Challenger and Colligan has not been made. For this further reason, Applicant respectfully submits that Claims 1 - 20 are patentably distinguished over Challenger and Colligan.

VIII. CLAIMS APPENDIX - 37 CFR § 41.37(c)(1)(viii)

A copy of the pending Claims involved in the appeal is attached as Appendix A.

IX. EVIDENCE APPENDIX - 37 CFR § 41.37(c)(1)(ix)

There is no additional evidence relied upon for this appeal.


X. RELATED PROCEEDINGS APPENDIX - 37 CFR § 41.37(c)(1)(x)

There are no related proceedings.

XI. CONCLUSION

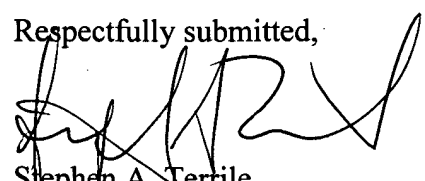
For the reasons set forth above, Applicant respectfully submits that the rejection of pending Claims 1 - 20 is unfounded, and requests that the rejection of Claims 1 - 20 be reversed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Mail Stop Appeal Brief – Patents, Board of Patent Appeals and Interferences, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450, on October 14, 2005.


Attorney for Applicant

10/14/05
Date of Signature

Respectfully submitted,


Stephen A. Terrile
Attorney for Applicant
Reg. No. 32,946

CLAIMS APPENDIX

1. A method for purchase verification, comprising the acts of:
receiving at a server a first message from a computer system, the first message including
a service tag, the service tag uniquely identifying the computer system;
determining at the server if the service tag is valid; and
generating a second message from the server, the second message authorizing providing a
benefit if the service tag is determined to be valid.
2. The method as recited in Claim 1, wherein the server includes a processor coupled
to a memory, further comprising the act of:
invalidating the service tag after generating the second message.
3. The method as recited in Claim 1, wherein the first message includes a product
code.
4. A method for purchase verification, comprising the acts of:
generating a service tag that uniquely identifies a computer system, the computer system
including a processor coupled to a memory;
storing the service tag in the memory at assembly of the computer system;
receiving a message at a server sent from the computer system, the message including the
service tag;
verifying that the service tag value as received matches a service tag value stored in the
server; and
authorizing receipt of a benefit if the received service tag matches.
5. The method as recited in Claim 4, wherein the service tag is stored as part of the
computer system basic input/output operating system.
6. The method as recited in Claim 4, further comprising the act of:
generating a second message, the message authorizing a purchaser to receive the benefit,
if the service tag matches.

7. The method as recited in Claim 5, wherein the benefit is Internet Service Provider service.

8. A method for purchase verification of a benefit, comprising the acts of:
receiving a first message at a first server, the first message being sent from a computer system, the first message including a service tag, the service tag uniquely identifying a computer system;
transmitting a second message from the first server to a second server, the second server attempting to verify the validity of the service tag; and
transmitting from the second server a third message to the first server, the third message allowing access to the benefit.

9. The method as recited in Claim 8, wherein the first message includes a product code.

10. The method as recited in Claim 8, further comprising the act of:
invalidating the service tag on the second server.

11. A system in a computer system for purchase verification, the computer system including a processor, the system comprising:
a non-volatile computer readable memory, the non-volatile computer readable memory including:
instructions, executable on the processor, configured to store a service tag installed upon assembly of the computer system, the service tag uniquely identifying the computer system; and
instructions, executable on the processor, configured to send the service tag to a remote server to verify the purchase of a benefit.

12. The system as recited in Claim 11, further comprising:
instructions, executable on the processor, configured to store a product code, the product code identifying the benefit.

13. The system as recited in Claim 11, further comprising:
instructions, executed on the processor, configured to communicate with a remote server,
the server having the ability to verify the service tag.

14. A system for purchase verification, the system being on a server platform, the
server operated by a service provider, the server configured to communicate with a purchased
computer system, the server including a processor and a memory, the server platform configured
to communicate with a remote computer system, the system comprising:

a non-volatile computer readable memory, the non-volatile computer readable memory
storing:

a database, the database including a set of valid service tags, the valid service tags
corresponding to computer systems that purchased a benefit; and
instructions, executable on the processor, configured to receive a message, the message
including a service tag, the service tag uniquely identifying a computer system.

15. The system as recited in Claim 14, further comprising:
instructions, executable on the processor, configured to receive a message, the message
including a product code.

16. The system as recited in Claim 15, further comprising:
instructions, executable on the processor, configured to authorize a purchaser to receive a
benefit.

17. The system as recited in Claim 14, further comprising:
instructions executable on the processor, configured to verify the service tag, wherein the
instructions to verify the service tag further comprise:
instructions to receive the service tag from the computer system;
instructions to recall the service tag stored in the server; and
instructions to compare the service tag received from the computer system to the
service tag recalled from the server to determine if the service tag received
from the computer system matches the service tag recalled from the
server.

18. The system as recited in Claim 17, further comprising:
instructions, executable on the processor, configured to authorize a purchaser to receive a benefit if the service tag received from the computer system matches the service tag recalled from the server.
19. The system recited in Claim 17, further comprising:
instructions, executable on the processor, configured to establish an internet service provider service account if the service tag received from a computer system matches the service tag recalled from the server.
20. The computer system as recited in Claim 17, further comprising:
instructions, executable on the processor, configured to invalidate the service tag stored in the memory of the server.

EVIDENCE APPENDIX

There is no additional evidence relied upon for this appeal.

RELATED PROCEEDINGS APPENDIX

There are no related proceedings.